REMARKS

Claims 1-37 are currently pending in this application. In the Office Action ("OA")[1] mailed February 8, 2006, the Examiner rejected claims 1-37 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,175,917 to Arrow ("*Arrow*") in view of U.S. Patent No. 6,751,729 to Giniger ("*Giniger*"). Applicant hereby amends claims 1, 7, 8, 14-17, 22, 27, 32, and 37. Support for the amendment of claims 1, 2, 7-9, 14-17, 22, and 37 can be found throughout the Drawings and the Specification at, for example, Figures 2, 4B, and 7-10, page 5, lines 8-17, page 12, lines 5-13, and page 15, lines 20-22. In view of the following remarks, Applicant respectfully traverses the Examiner's rejection of the claims under 35 U.S.C. § 103(a).

Rejection of claims 1-37 under 35 U.S.C. § 103(a)

To establish a prima facie case of obviousness, three basic criteria must be met. First, the prior art reference as modified must teach or suggest all the claim elements. (See M.P.E.P. § 2143.03 (8th ed. 2001)). Second, there must be some suggestion or motivation, either in the reference or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings. (See M.P.E.P. § 2143 (8th ed. 2001)). Third a reasonable expectation of success must exist. Moreover, each of these requirement must "be found in the prior art, and not be based on applicant's disclosure." (M.P.E.P. § 2143.03 (8th ed. 2001)).

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

As noted above, the Examiner rejected claims 1-37 under 35 U.S.C. § 103(a) as being unpatentable over *Arrow* in view of *Giniger*. *Arrow* discloses a method and system for swapping a computer operating system (*Arrow* title). *Arrow* selectively switches between storage memories via commands received over a virtual private network ("VPN") so that a VPN unit may be selectively booted with an alternate operating system program (*Arrow* col. 3, lines 2-20; col. 3, lines 35-40). Data packets are encapsulated in accordance with the Internet Protocol and transmitted from one member of a VPN to another member of the same VPN over a public data network (*Arrow* fig. 2; col. 7, lines 13-17). In *Arrow*, "RSA module 722 provides public key/private key security functions," and "[k]ey management module 738 sets up keys for encryption and authentication functions" (*Arrow* col. 11, lines 24-34). Moreover, in *Arrow*, an "NSID, or name space ID [which] is the MD5 hash of a user name," and an "MKID[, which] is the master key ID of the domain... serve to identify the remote client" (*Arrow* col. 15, lines 25-28).

In contrast, the claimed invention as demonstrated, for example in proposed claim 1, recites the step of "receiving a non-tunneled packet from a source node in the first private network" and "acquiring a channel key associated with a channel based on the determination, wherein the channel comprises a plurality of non-tunneled virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, wherein only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated upon an addition of a new channel node to the channel, and wherein the channel key is updated upon a departure of one of the channel nodes from the

channel." *Arrow* teaches using "public key/private key security functions" and "[k]ey management module 738" that "sets up keys for encryption and authentication functions" for sending data through tunnels in a virtual private network (*Arrow* col. 6, lines 1-4; col. 11, lines 24-34). *Arrow* also teaches an "NSID" and an "MKID" that "serve to identify the remote client" (*Arrow* col. 15, lines 25-28). However, the use of public key/private key security functions, and the use of NSID and MKID to identify a remote client and to send data through tunnels in a virtual network, as disclosed in *Arrow*, are not sufficient to constitute the aforementioned "receiving" and "acquiring," as recited in proposed claim 1. Moreover, the Examiner admitted that *Arrow* does not explicitly disclose that "the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes can communicate over the channel" (OA page 3, lines 5-9 and Inquiry). Instead, the Examiner alleged that *Giniger* teaches those features.

Giniger is not sufficient to make up for the deficiencies of *Arrow*. *Giniger* discloses an automated operation and security system for virtual private networks (*Giniger* title) that authenticates a "node device by the server" by "encoding a message using the stored private key at the node device, sending the encoded message to the server, and decoding the message using the public key for the node device that was provided to the server" (*Giniger* col. 5, lines 6-10). Furthermore, a "key exchange module 410 is used to exchange cryptographic keys with other computers or devices on Internet 100 in order to establish secure tunnels with those computers or devices" (*Giniger* col. 11, lines 55-58). In *Giniger*, "each edge device maintains a secure

communication tunnel with generally one or more other edge devices over which the edge devices securely transfer communications" (*Giniger* col. 7, lines 37-40), and an edge device "passes the communication through the tunnel to its destination" (*Giniger* col. 7, lines 59-64). *Giniger*, however, does not disclose "receiving a non-tunneled packet from a source node in the first private network" and "acquiring a channel key associated with a channel based on the determination, wherein the channel comprises a plurality of non-tunneled virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, wherein only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated upon an addition of a new channel node to the channel, and wherein the channel key is updated upon a departure of one of the channel nodes from the channel" (emphasis added), as recited in proposed claim 1.

Neither *Arrow* nor *Giniger*, taken alone or in any reasonable combination, teach or suggest each and every element recited in proposed claim 1. For at least this reason, a prima facie case of obviousness has not been established with respect to proposed claim 1. Accordingly, Applicant requests withdrawal of the rejection under 35 U.S.C. § 103(a) and the timely allowance of claim 1. Because claims 7, 8, 14-17, 22, 27, 32, and 37 are independent claims with limitations similar to those of claim 1, Applicant further submits that the rejections of claims 7, 8, 14-17, 22, 27, 32, and 37 are not supported by *Arrow* in view of *Giniger*, for at least the reasons given with respect to proposed claim 1. Accordingly, Applicant requests withdrawal of the rejection under 35 U.S.C. § 103(a) and the timely allowance of claims 7, 8, 14-17, 22, 27, 32, and 37.

The rejections of dependent claims 2-6, 9-13, 18-21, 23-26, 28-31, and 33-36 are unsupportable for the reasons stated above with regard to their respective allowable base claims. Accordingly, Applicant requests withdrawal of the rejection under 35 U.S.C. § 103(a) and the timely allowance of claims 2-6, 9-13, 18-21, 23-26, 28-31, and 33-36.

Conclusion

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: May 8, 2006

By: _____
Joshua Liu
Reg. No. 55,391